Ranking Member Yvette D. Clarke (D-NY) Opening Statement

Subcommittee on Counterterrorism and Intelligence and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies Joint Hearing

"Assessing Persistent and Emerging Cyber Threats to the U.S. Homeland"

May 21, 2014 at 10 AM

We all know that threats to systems supporting U.S. critical infrastructure, and federal and corporate information systems are evolving and growing. Advanced persistent threats—where adversaries possess sophisticated levels of expertise and significant---pose increasing risks.

Soon after his election in 2008, President Obama declared the cyber threat to be "one of the most serious economic and national security challenges we face as a nation" and stated "America's economic prosperity in the 21st century will depend on cybersecurity." The Director of National Intelligence has also warned of the increasing globalization of cyber attacks, including those carried out by foreign militaries or organized international crime.

On Monday, we saw the Department of Justice indict members of a foreign military involved in economic espionage cyber crime, most likely espionage in support of its state-owned companies. It appears that the Department of Justice has been working on this indictment for more than a year. Prosecutors in the DOJ's National Security Division had to show there was strong, specific evidence, and there had to be companies that were willing to go public against China.

The evolving array of cyber-based threats facing the nation poses threats to national security, commerce and intellectual property, and individuals. Intentional threats include both targeted and untargeted attacks from a variety of sources. These sources include business competitors, criminal groups, hackers, and foreign nations engaged in espionage and information warfare.

These sources of cybersecurity threats make use of various techniques to compromise information or adversely affect computers, software, a network, an organization's operation, an industry, or the Internet itself. Such threat sources vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. Adversarial cybersecurity threats can range from, as I like to say, "From Botnets to Business Competitors".

Addressing international cybercrime threats involves many government and private entities—including Internet service providers, security vendors, software developers, and computer forensics specialists. Their focus is on developing and implementing technology systems to protect against computer intrusions, Internet fraud, and spam and, if a crime does occur, detecting it and helping to gather evidence for an investigation.

Also, because cybercrime threats cross national and state borders, law enforcement organizations have to deal with multiple jurisdictions with their own laws and legal procedures, a situation that complicates and hobbles investigations. Law enforcement's challenge in investigating and prosecuting malicious, 21st Century cybercriminals is this---modern criminals can readily leverage technology to victimize targets across borders, and the criminals themselves need not cross a single border to do so.

This creates a unique test in identifying and locating the criminals, and in apprehending and prosecuting them. The United States has extradition treaties and mutual legal assistance agreements with some, but not all countries. And, even with these agreements in place, the process may be slow.

We must continue to search for ways that Congress can help enhance international law enforcement capabilities and to get criminals off the streets, or shall we say, out of cyberspace, and thus protect U.S. critical infrastructure, government systems, companies, and consumers.